MF0490_3: Gestión de servicios en el sistema informático

Elaborado por: María Victoria Pequeño Collado

Edición: 5.0

EDITORIAL ELEARNING S.L.

ISBN: 978-84-16424-64-1 • Depósito legal: MA 723-2015

Impreso en España - Printed in Spain

Presentación

Identificación del Módulo Formativo

Bienvenido al Módulo Formativo **MF0490_3: Gestión de servicios en el sistema informático**. Este módulo formativo pertenece a los certificados de profesionalidad **IFCT0509: Administración de Servicios de Internet** y, que pertenecen a la familia de Informática y Comunicaciones.

Presentación de los contenidos

La finalidad de este Módulo Formativo es enseñar al alumno a gestionar servicios en el sistema informático.

Para ello, en primer lugar se analizará la gestión de la seguridad y normativas, el análisis de los procesos de sistemas, la demostración de sistemas de almacenamiento y la utilización de métricas e indicadores de monitorización de rendimiento de sistemas. También se estudiará la confección del proceso de monitorización de sistemas y comunicaciones, la selección del sistema de registro de en función de los requerimientos de la organización, y por último, se profundizará en la administración del control de accesos adecuados de los sistemas de información.

Objetivos del Módulo Formativo

Al finalizar este Módulo Formativo aprenderás a:

– Analizar los procesos del sistema con objeto de asegurar un rendimiento adecuado a los parámetros especificados en el plan de explotación.

– Aplicar procedimientos de administración a dispositivos de almacenamiento para ofrecer al usuario un sistema de registro de la información íntegro, seguro y disponible.

– Administrar el acceso al sistema y a los recursos para verificar el uso adecuado y seguro de los mismos.

– Evaluar el uso y rendimiento de los servicios de comunicaciones para mantenerlos dentro de los parámetros especificados.

Índice

UD1

Gestión de la seguridad y normativas

1.1. Norma ISO 27002 Código de buenas prácticas para la gestión de la seguridad de la información

1.2. Metodología ITIL Librería de infraestructuras de las tecnologías de la información

1.3. Ley orgánica de Protección de datos de carácter personal

1.4. Normativas más frecuentemente utilizadas para la gestión de la seguridad física

1.1. Norma ISO 27002 Código de buenas prácticas para la gestión de la seguridad de la información

"La Información es poder" ¿Cuántas veces no hemos escuchado esta frase? Fue ya hace unos años, con la aparición de las nuevas tecnologías, cuando se empezó a hablar de Sociedad de la Información. Tener la opción de adquirir información y poder transmitirla de una forma eficaz y eficiente revolucionó a la sociedad y la manera de hacer las cosas. Y la cosa no se quedó ahí, este concepto evolucionó hasta la idea de Sociedad del Conocimiento actual, donde no sólo es importante la adquisición y transmisión de la información, sino aún lo es más la capacidad para transformarla y utilizarla.

En este contexto, la accesibilidad y disponibilidad de la Información, se ha convertido para las empresas tanto en su mayor activo como en su mayor riesgo. Una empresa manejará muchísima información, independientemente del formato o del tipo del que esta sea, que es lo que le aporta realmente valor a la misma, diferenciándola de las demás y ayudándola a conseguir sus objetivos, y que por lo tanto, deberá proteger al máximo para hacerla lo menos vulnerable posible a cualquier amenaza, tanto interna como externa, que pueda poner en peligro la integridad de la misma.

Al final, toda empresa y organización comparten un proceso común para la consecución de sus objetivos: ciertos datos de entrada procesados de cierta forma dan como resultado una información que se convierten en el principal activo de la organización y que hay que mantener integra, disponible y de forma confidencial para asegurar una posición competitiva frente al resto de

empresas, que a su vez no haga obtener la rentabilidad necesaria y de manera que cumplamos la normativa legal al respecto.

Y es precisamente el desarrollo creciente de las nuevas tecnologías el que hace que el riesgo de amenazas para la información de las organizaciones esté creciendo de forma exponencial, dado que estas aprovecharán cualquier vulnerabilidad para acceder a nuestra información, pudiendo dar lugar a fraude, actos de vandalismo informático e incluso espionaje industrial, con las pérdidas de rentabilidad y de posicionamiento en las que esto puede derivar.

Es por ello fundamental proteger la información, porque no sólo con actos intencionados podemos vulnerarla, si no que actuaciones involuntarias también pueden alterarla y hacerla accesible, y para ello actualmente contamos con una herramienta de gran utilidad y ayuda en la gestión de cualquier organización, los Sistemas de Gestión de la Seguridad de la Información (SGSI).

Definición

El Sistemas de Gestión de la Seguridad de la Información (SGSI) es una herramienta que nos va a permitir conocer, gestionar y minimizar los riesgos que amenacen la seguridad de la información dentro de nuestra organización. Esto debe hacerse mediante un proceso sistemático, documentado y conocido por toda la organización y es este proceso el que constituye el SGSI.

Su fin último es proteger a las organizaciones frente a posibles amenazas que pongan en riesgo su viabilidad y rentabilidad y hacerlo dentro de la legalidad.

En definitiva, hacer que el riesgo al que está sometido la información de las organizaciones se sitúe por debajo del nivel que la propia organización estime como asumible.

El Sistema de Gestión de la Seguridad de la Información implantado nos deberá permitir:

– Analizar y Ordenar nuestros sistemas de información

– Definir los procesos de trabajo

– Medir la eficacia de las medidas tomadas para minimizar los riesgos.

¿Y cuál es la razón para que la gestión de la seguridad de la información se realice mediante procesos? Simplemente que los medios técnicos no son capaces por si solos, ya que técnicamente es imposible, de garantizar un nivel de seguridad tal que satisfaga todas las necesidades de la organización. Para llevar a cabo una gestión lo más eficiente posible de la seguridad todos los miembros de la organización, así como clientes o proveedores externos a ella deben colaborar, participar e involucrarse en el proceso y esto sólo es posible si el procedimiento a seguir para saber cómo actuar y que está o no está permitido es conocido y participado por todos los actores que participan en el proceso.

Sabías qué

ISMS (Information Security Management System) son las siglas que se utilizan en inglés para definir a los Sistemas de Gestión de la Seguridad de la Información, por lo que te encontrarás este término en mucha bibliografía o documentación que verse sobre este tema.

La información que intenta proteger el SGSI es de muy diversa índole, puede tratarse de correos electrónicos, imágenes, bases de datos de clientes, páginas web, contratos, documentación técnica, listados , Curriculum Vitae del personal, etc., y puede llegar desde distintas fuentes, tanto externas como internas a la organización. Así mismo, para definir el sistema, también tenemos que tener en cuenta que la información puede estar soportada por distintos medios, ya sea papel u otros medios digitales.

Conocer el ciclo de vida de la información también es importante, porque nos permitirá definir cuál es la importancia de la información en cada momento (algo que ahora es muy importante y primordial proteger quizá no lo es tanto en otro momento de su ciclo de vida). Normalmente, es el que se detalla en la figura adjunta:

La información se crea, se guarda, se utiliza, se comparte, se archiva y se destruye y el SGSI nos marcará los procedimientos y políticas que nos garanticen que durante todas estas etapas la confidencialidad, integridad y disponibilidad de la información se mantenga minimizando al máximo los riesgos de seguridad:

– Confidencialidad: se dará siempre que la información no sea puesta a disposición ni sea revelada a aquellas personas físicas, o procesos, que no estén autorizados para poseerla.

– Integridad: una información será integra cuando mantenga a lo largo de todo su ciclo de vida la exactitud y la plenitud de su inicio.

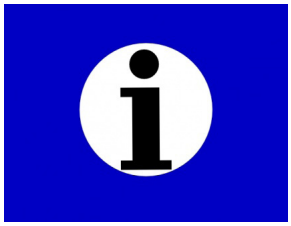
– Disponibilidad: la información debe estar disponible siempre que sea requerida por un usuario que tenga autorizado el acceso a ella.

Importante

Estos parámetros (confidencialidad, integridad y disponibilidad) son los parámetros básicos de la seguridad de la información, y para identificarlos se utiliza el acrónimo CID.

Recuerda

La información que le resulta imprescindible a la empresa para su funcionamiento se denomina activo de seguridad de la información, y su protección es el principal objetivo de un SGSI.



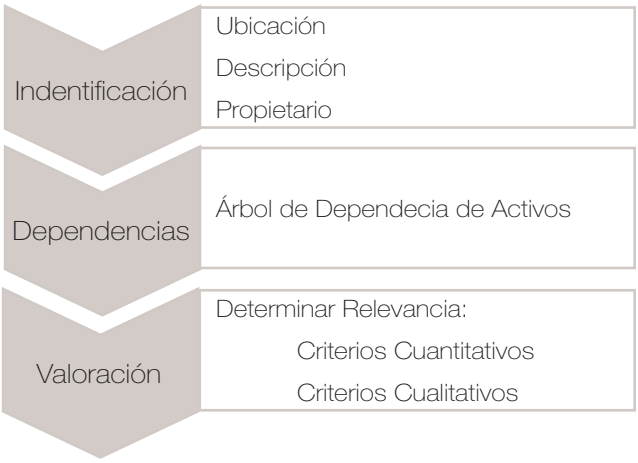
En función de la naturaleza de esta información podemos dividir estos activos de la Seguridad de la Información en varios grupos, la forma de proteger unos u otros activos requerirá procedimientos distintos. Así nos encontraremos con:

– Servicio: son los procesos que la organización ofrece al exterior e incluso en algunos casos, como las gestión de nóminas, internamente

– Datos e Información: son el centro del SGSI. El resto de activos darán soporte para manipularla, almacenarla, distribuirla, etc.

- Aplicaciones de Software: nos permiten tratar la información y los datos
- Equipos informáticos: en ellos se almacena la información y a través de ellos se gestiona
- Personal: es el activo principal, puesto que es el encargado de manipular la información y aplicar las normas que nos imponga el SGSI.
- Redes de Comunicación: hacen posible el movimiento de la información.
- Soportes de Información: son los soportes físicos que permiten el almacenamiento de la información.
- Equipos auxiliares: estará constituido por todos los equipos de la organización que no se han incluido en ningún otro activo, como impresosoras, equipos de climatización, etc.
- Instalaciones: este activo hace referencia a las instalaciones donde se alojan los sistemas de información. Su protección entrará dentro de la Seguridad Física, a diferencia de los otros activos que estarán dentro de la Seguridad Lógica de la Seguridad Informática.
- Activos intangibles: imagen y reputación de la empresa

Conocer cada uno de estos activos e identificarlos conociendo su ubicación, su descripción y a quién se le considera propietario, es el primer paso para poder protegerlos. Por ejemplo, el propietario del activo es quien debe definir el grado de seguridad que su activo debe poseer, porque es él quien conoce su valor para la organización. A continuación de la identificación hay que determinar si existe alguna dependencia entre ellos, puesto que si las hay la seguridad y protección de uno de los activos puede comprometer la de otros, hay por lo tanto que construir un árbol de dependencia de activos, en el que se reflejará las interdependencias entre los activos, desde los que estén más arriba en cuanto a nivel de seguridad se refiere, hasta los que estén más abajo. El siguiente paso es la determinación de la relevancia de los activos para poder determinar el nivel de seguridad que se le ha de aplicar a cada uno en función de la importancia que tenga su vulnerabilidad. Esta valoración puede realizarse atendiendo a criterios cuantitativos (por su valor económico) o atendiendo a criterios cualitativos (normalmente basado en las CID).



De la necesidad de poseer unas políticas y procedimientos utilizables por cualquier organización buscando la forma adecuada de gestionar temas relativos a la gestión de la información, nació un conjunto de estándares bajo el nombre de ISO /IEC 27000.

Las normas descritas bajo estos estándares nos van a permitirán reducir el posible impacto de los posibles riesgos a los que está sometida la información de nuestra organización sin tener que hacer grandes inversiones y sin la necesidad de contar con una amplia estructura de personal.

La ISO/IEC 27000 está formada por una familia de normas, todas las cuales hablan sobre la gestión de la información, y definen conceptos y procedimientos en relación a ello. A continuación se muestra una tabla que contiene el listado de normas que forman la familia y el título de cada una de ellas, que nos dará una idea de que parte de los Sistemas de Gestión de la Información aborda:

– ISO 27000

  Gestión de la Seguridad de la Información: fundamentos y vocabulario. Incluye una visión general de todas las normas de la familia, además de recoger aquellos términos y definiciones que en ellas se emplearán.

– ISO 27001

  Especificaciones para un SGSI. Se trata de la norma principal de la familia. En ella se definen los procedimientos para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un SGSI. Con esta norma

se certificarán las organizaciones que deseen certificar sus Sistemas de Gestión de Seguridad de la Información.

– ISO 27002

  Código de Buenas Prácticas: en ella se recogen los procedimientos para asegurar los sistemas de información de una organización, describiendo distintas áreas de actuación, que incluirán distintos aspectos a asegurar dentro de cada uno y que a su vez contendrán mecanismos para asegurar los distintos aspectos a asegurar.

– ISO 27003

  Guía de Implantación de un SGSI.

– ISO 27004

  Sistema de Métricas e Indicadores.

– ISO 27005

  Guía de Análisis y Gestión de Riesgos.

– ISO 27006

  Especificaciones para Organismos Certificadores de SGSI.

– ISO 27007

  Guía para auditar un SGSI.

– ISO 2701X

  Guías sectoriales.

– ISO 27XXX

  Futuras normas.

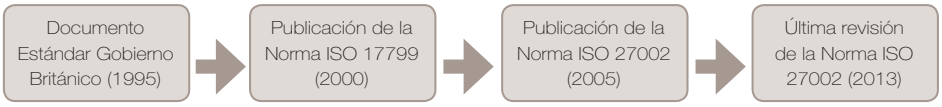
De todas ellas, la Norma ISO 27002 (Código de buenas prácticas para la gestión de la Seguridad de la información) es la que aquí nos ocupa y la que propone los controles a los que tenemos que someter a los activos de nuestro sistema para intentar asegurar que los riesgos a los que están sometidos se reducen al nivel que el propietario de los activos considera como aceptable, y como todos los estándares, son de aplicación voluntaria, aunque su aplicación, además de contribuir a una considerable mejora de la calidad y de la

seguridad de muchos productos y servicios también facilita el mejor entendimiento entre distintas organizaciones.

Importante

En la Norma ISO 27002 se recogen los procedimientos para asegurar los sistemas de información de una organización, describiendo distintas áreas de actuación, que incluirán distintos aspectos a asegurar dentro de cada uno y que a su vez contendrán mecanismos para asegurar los distintos aspectos a asegurar.

Originalmente esta norma se publicó en el 2005 como un cambio de nombre de la norma ISO 17799, que a su vez estaba basada en un documento que el Gobierno inglés había tomado como estándar y que fue publicada como norma en el año 2000. La última revisión de la norma se produce en el 2013. Esta norma se utiliza de forma complementaría con la ISO 27001, que como vimos en la tabla anterior es la principal de la familia y la que describe los procedimientos para la implantación del Sistema de Seguridad de la Información.



Definición

Definiremos a los Sistemas de Información (cuyo aseguramiento frente a los distintos riesgos es el objeto de los controles propuestos en la Norma 27200) a los soportes de almacenamiento, redes de datos y equipos informáticos en los que reside la información que pretende proteger el SGSI.

Como comentamos anteriormente es necesario conocer los riesgos a los que están sometidos nuestros activos para poder reducirlos, o determinar cuál es el riesgo que estamos dispuestos a asumir. Para ello las organizaciones, cuando están implementando un SGSI, en su fase de planificación realizará un Análisis de Riesgo, que determinará a que amenazas están expuestos los ac-

tivos que pretendemos proteger y se determinará como se gestionarán estos riesgos para minimizarlos todo lo posible.

Por lo tanto con el resultado del Análisis y Gestión de Riesgos podremos ya establecer ciertos controles que nos permitan reducir estos riesgos, y las Norma ISO27002 nos ofrecerá una guía de Buenas

Prácticas en la que se recogerán aquellas recomendaciones y controles que nos van a permitir llegar a cabo el aseguramiento de nuestros sistemas de información.

La norma define 11 categorías distintas de seguridad, en las que se engloban 39 objetivos o aspectos a asegurar en nuestros sistemas y 133 controles que nos van a permitir asegurar estos aspectos.

A continuación se detallarán en una tabla cada una de las áreas de actuación, así como los Objetivos de Control y los distintos controles que recoge la norma ISO 27002, y aunque conocer cuáles existen para tener la opción de conocerlos nunca está de más, profundizar en detalle de cada uno de estos controles escapa del ámbito de este contenido. Aun así antes de enumerar el listado de controles vamos a ver unas pinceladas de cada una de las áreas de Actuación, o categorías de seguridad, que recoge la norma:

– Política de Seguridad. Establece que se ha de generar un documento denominado Política de Seguridad de la Información, en el que se establecerán las directrices y que servirá de soporte para la seguridad de la información, teniendo siempre presente tanto la ley y la regulación vigente.

– Aspectos organizativos de la seguridad de la información. Se manejan en este área los aspectos relativos a como se debe gestionar y manejar la seguridad de la información, tanto por las personas ajenas a la organización que acceden a ella como a la organización interna.

– Gestión de activos. Se establecen en esta área los controles para la protección de los activos de la organización, para ello establece la necesidad de crear inventario de los activos, indicando su uso, su propiedad y su clasificación.

– Seguridad ligada a los recursos humanos. Nos hemos de intentar asegurar que todos las personas relacionadas con la empresa, personal interno, proveedores y otros, entiendan sus responsabilidades y sean las personas adecuadas para el puesto para minimizar en la medida de lo posible el mal uso de la información.